

REMARKS

Claims 1-5 and 7-37 are all the claims presently pending in the application. Claims 1, 5, 7-19, and 21-36 are amended to more clearly define the invention and claim 37 is added. Claims 1, 29, 31, 33, and 35 are independent.

These amendments are made only to more particularly point out the invention for the Examiner and not for narrowing the scope of the claims or for any reason related to a statutory requirement for patentability.

Applicants also note that, notwithstanding any claim amendments herein or later during prosecution, Applicants' intent is to encompass equivalents of all claim elements.

Applicants gratefully acknowledge that claims 17, and 24-26 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. However, Applicants respectfully submit that all of the claims are allowable.

Claims 1-12, 15, 18, 20, and 27-36 stand rejected under 35 U.S.C. § 102(b) as being anticipated by the Ginter et al. reference. Claims 13-14, and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Ginter et al. reference in view of the Al-Salqan reference.

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

An exemplary embodiment of the claimed invention, as recited by, for example, independent claim 1, is directed to a method for storing information in a recoverable manner on an untrusted system. The method includes sending a request from a client to a recovery server,

determining whether the request is legitimate, sending an old local key to the client based on the determination, decrypting the failed database with the old local key at the client to recover a failed database, and re-encrypting the recovered database with a new local key. At least one of the old local key and the new local key is based upon at least one unique characteristic of a hardware component associated with the database.

Conventional distribute applications handle data on untrusted systems. These applications conventionally use a protection scheme that encrypts the data and which requires the use of a key to access the data. However, such conventional systems have a problem where a client may provide the keys to an unauthorized client.

In stark contrast to these conventional systems, the present invention provides the ability to protect the data resident on an untrusted system by providing a key that is based upon at least one unique characteristic of a hardware component associated with the database. In this manner, the present invention prevents the database from being accessed on an unauthorized client.

II. THE PRIOR ART REJECTIONS

A. The 102(b) Ginter et al. reference rejection

Regarding the rejection of claims 1-12, 15, 18, 20, and 27-36, the Examiner alleges that the Ginter et al. reference teaches the claimed invention. Applicants submit, however, that there are elements of the claimed invention which are neither taught nor suggested by the Ginter et al. reference.

None of the applied references teaches or suggests the features of the claimed invention

including at least one of the old local key and the new local key being based upon at least one unique characteristic of a hardware component associated with the database.

Rather, and in stark contrast, the Ginter et al. reference discloses changing and/or convolving tags which may include encryption keys and/or securing techniques. (Col. 215, line 64 - col. 216 - line 17). While the Ginter et al. reference discloses a “hardware SPE”, that disclosure is merely to distinguish between a hardware based secure event processing environment which includes security features that are entirely incorporated into features in hardware and a software based host event processing environment which includes security features that are entirely incorporated into features in software (Fig. 10; col. 79, line 5 - col. 80, line 61).

There is no disclosure anywhere within any of the applied references of any key at all that is based upon a unique characteristic of a hardware component associated with a database.

The Ginter et al. reference discloses that keys are specific to the type of encryption being supported (col. 119, lines 27-31). That these keys may be adjusted or convolved to yield new keys (col. 119, lines 59-64).

While the Ginter et al. reference appears to disclose basing a key upon a site identification (col. 120, lines 1-3), using a hardware-based random number generator (col. 201, lines 1-20), using unpredictable external events such as disk I/O timing and/or keystrokes on a keyboard (col. 201, lines 21-26), aging and/or convolving the keys (col. 203, line 38 - col. 207, line 48), the Ginter et al. reference does not disclose basing a key upon a characteristic of hardware, let alone hardware associated with a database.

Further, the approach that is disclosed by the Ginter et al. reference regarding key convolution is fundamentally different than the present invention. The Ginter et al. reference has an object to make a key interchangeable between different VDUs. In column 203, lines 39-56, the Ginter et al. reference explains that the key convolution process is designed to allow key sharing between VDUs. Thus, the Ginter et al. reference teaches that the key can be shared among VDUs that have the same Site ID and within the time expiration period.

In stark contrast, the present invention provides a completely different approach. In particular, the present invention relies upon the characteristics of the hardware of the local machine to derive the key database master key. Thus, any attempt to share the key database will cause the decryption of the key database to fail on a different machine. Therefore, the present invention makes the key database very hard to move because if a key database is moved, the end user will have to go through the recovery flow in order to obtain access to the database.

In review, an exemplary embodiment of the present invention secures a database using a key that is based upon a hardware characteristic. The Ginter et al. reference describes the components of a secure processing unit at col. 68, lines 19-36 with reference to Figure 9. However, the Ginter et al. reference does not teach or suggest anything at all regarding a key that may be based upon a hardware characteristic.

Therefore, the Ginter et al. reference does not teach or suggest each and every element of the claimed invention and the Examiner is respectfully requested to withdraw this rejection of claims 1-12, 15, 18, 20, and 27-36.

B. The Ginter et al. reference in view of the Al-Salqan reference

Regarding the rejection of claims 13-14 and 16, the Examiner alleges that the Al-Salqan reference would have been combined with the Ginter et al. reference to form the claimed invention. Applicants submit, however, that these references would not have been combined and even if combined, the combination would not teach or suggest each and every element of the claimed invention.

Applicants submits that these references would not have been combined as alleged by the Examiner. Indeed, the references are directed to completely different matters and problems.

Specifically, the Ginter et al. reference is directed to systems and methods for secure transaction management and for protecting the rights of various participants in electronic commerce or electronically-facilitated transactions (col. 1, lines 11-40). In other words, the Ginter et al. reference is directed to an end user that is not implicitly trusted because that user might be tampering with the system.

In stark contrast, the Al-Salqan reference is directed to the completely different and unrelated problem of the recovery of cryptographic keys. (Col. 2, lines 42 - 47). In other words, the Al-Salqan reference assumes that the end user is an implicitly trusted user that has forgotten or misplaced the password and would like to recover it using a secret pass phrase or other proof of authorization (e.g., by providing a mother's maiden name, a social security number or the like).

One of ordinary skill in the art who was concerned with ensuring secure transaction management and protection of rights as the Ginter et al. reference is concerned with addressing

would not have referred to the Al-Salqan reference because the Al-Salqan reference is directed to the completely different and unrelated problem of the recovery of keys which have become lost and/or inaccessible because an authorized person is not available. Thus, the references would not have been combined.

Moreover, even assuming arguendo that one of ordinary skill in the art would have been motivated to combine these references, the combination would not teach or suggest each and every element of the claimed invention.

As explained above, the Ginter et al. reference does not teach or suggest at least one of a old local key and a new local key being based upon at least one unique characteristic of a hardware component associated with the database.

The Al-Salqan reference does not remedy this deficiency.

Indeed, the Examiner does not allege that the Al-Salqan reference discloses these features.

Lastly, regarding the means plus function recitations, the Examiner has failed to interpret the claims to read only on the structures or materials disclosed in the specification and “equivalents thereof.” The Federal Circuit has made it clear that the Office is required to interpret means plus function language in accordance with 35 U.S.C. § 112, sixth paragraph (see M.P.E.P. §2106; *In re Donaldson*, 16 F.3d 1189, 1193 (Fed. Cir. 1994) and *In re Alappat*, 33 F.3d 1526, 1540 (Fed. Cir. 1994)). Clearly, the Examiner has failed to interpret the claims to read only on the structures or materials disclosed by the present specification and “equivalents thereof.”

Therefore, the Examiner is respectfully requested to withdraw the rejection of claims 13-14 and 16.

III. FORMAL MATTERS AND CONCLUSION

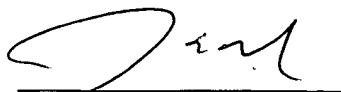
In view of the foregoing amendments and remarks, Applicants respectfully submit that claims 1-5 and 7-37, all the claims presently pending in the Application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the Application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 09-0441.

Respectfully Submitted,

Date: 11/22/04


James E. Howard
Registration No. 39,715

McGinn & Gibb, PLLC
8321 Old Courthouse Rd., Suite 200
Vienna, Virginia 22182
(703) 761-4100
Customer No. 21254